INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

"CLOUD SECURITY: CONTROLS AND ISSUES"

CHAITANYA N. GADGE, PROF. S. T. KHANDARE

1. ME (appeared), BNCOE, PUSAD
2. Associate Professor, BNCOE, PUSAD

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Cloud Security

Corrective Controls

Virtualizing Security

Auditability

No Security Perimeter

Community

Corresponding Author

Mr. Chaitanya N. Gadge

Abstract

In this paper we mostly concentrated on different security issues and security controls in cloud. Cloud security basically not any application software that can be offered or given as cloud based. We can say that it is one of important service provided by "The Cloud". Hence We can argue that "Security as a service" usually refers to security services provided by a third party using the other service model, but there's a compelling set of capabilities that enables companies large and small to be both effective, efficient and cost-manageable as we embrace the "new" world of highly distributed applications, content and communications .[1] As with virtualization, when we discuss "security" and "cloud computing," any of the three services often are conflated such as Software as a service (SaaS). Platform as a service (PaaS). Infrastructure as a service (IaaS).There are a lot of securities issues/concerns associated with cloud computing. Security issues are mostly divided into two groups. Security issues faced by cloud providers that provide different services to the customer and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. [2]There are also different security controls present to prevent the customer's security policies such as .preventative controls, corrective controls, etc.

INTRODUCTION

Cloud computing security (sometimes referred to simply as "cloud security") is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

"Cloud computing" as "the logical computational resources (data, software) accessible via a computer network (through WAN or Internet etc.), rather than from a local computer. Managing local computers is hard: there are security issues, computer lifecycle issues, accessibility issues. Cloud computing, ideally is easy: use it and leave it, access your data from anywhere over world. To end users, whether individuals or companies, "the cloud" is an abstraction, a computing environment that can expand to suit users' needs.

Basically**, Cloud computing** is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There is different cloud models, deployment models used for security purpose.

Cloud computing deployment models

1 **Cloud computing service models**

Software as a Service (SaaS) provides a number of ways to control access to the Web portal, such as the management of user identities, application level configuration, and the ability to restrict access to specific IP address ranges or geographies.

Platform as a Service (PaaS) allow clients to assume more responsibilities for managing the configuration and security for the middleware, database software, and application runtime environments**. Infrastructure as a Service (IaaS)** model transfers even more control, and responsibility for security, from the Cloud provider to the client; access is available to the operating system that supports virtual images, networking, and storage [3].

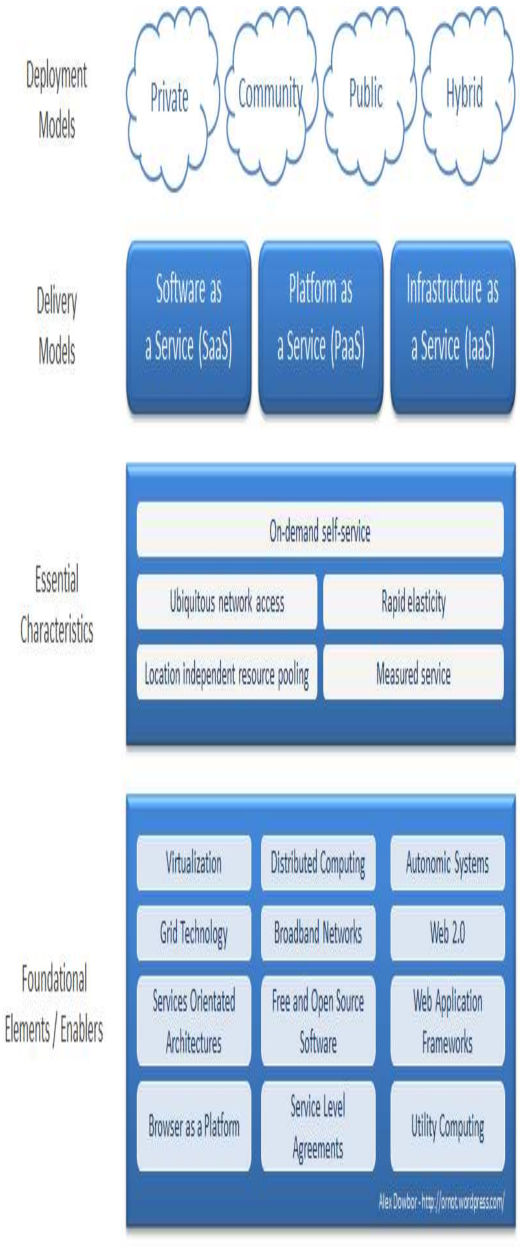
1. Public Cloud - A public cloud can be accessed by any subscriber with an

internet connection and access to the cloud space.

2. Private Cloud - A private cloud is established for a specific group or organization and limits access to just that group.

3. Community Cloud - A community cloud is shared among two or more organizations that have similar cloud requirements.

4. Hybrid Cloud - A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community. [4]


Deployment Models
Private
Community
Public
Hybrid
Delivery Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Essential Characteristics
On-demand self-service
Ubiquitous network access
Rapid elasticity
Location independent resource pooling
Measured service
Foundational Elements / Enablers
Virtualization
Distributed Computing
Autonomic Systems
Grid Technology
Broadband Networks
Web 2.0
Services Orientated Architectures
Free and Open Source Software
Web Application Frameworks
Browser as a Platform
Service Level Agreements
Utility Computing
Alex Dowbor - http://ornot.wordpress.com/

Based on the NIST Working Definition of Cloud Computing v14 and http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

Creative Commons Attribution-Share Alike 3.0
Alexander Dowbor – http://ornot.wordpress.com

FIG.1 Visual Model of Cloud Computing

CONTROLS

There are different types included in cloud controls that are classified as follows:
• Preventative controls exist to prevent the threat from coming in contact with the weakness
• Detective controls exist to identify that the threat has landed in our systems.
• Corrective controls exist to mitigate or lessen the effects of the threat being manifested.

- Deterrent Control is to reduce the likelihood of a Vulnerability being exploited without actually reducing the exposure.

• Corrective controls

As a result, Corrective Controls are all about reducing the Impact of the exploited Vulnerability rather than preventing them from happening in the first place. The key point here is that the attack has already begun and all we can do is limit the severity of it.

Looking at the Impact assessment, it is entirely dependent on the number of Information Assets that are exposed. The goal of the Corrective Control, therefore, should be to reduce the quantity of Information Assets that are exposed. This will be entirely dependent on the nature of the Vulnerability, however something as simple as terminating the associated users session may be enough to limit the number of records they were able to steal or modify.

- **Deterrent Controls**

Deterrent Controls are that they do not attempt to fix the associated Vulnerability; they just attempt to make it occur less frequently. The goal of a Deterrent Control is to reduce the likelihood of a Vulnerability being exploited without actually reducing the exposure.

Deterrent controls are used in phishing attack, which is completely outside of the control of the target company, is successful by increasing the awareness of its customers. Similarly, for internal facing threats, including black lists of known malware sites and so forth can reduce the likelihood of staff being exposed to these kinds of threats. There are many tips on the OWASP phishing page on how to address phishing type threats, where your only options are deterrent controls.[5]

- **Detective controls**

Detective controls are measures a company uses to identify irregularities so they can be corrected, ideally as promptly as possible. Laws like the Sarbanes-Oxley Act of 2002 mandate the use of internal controls to address common accounting and ethics problems, and companies also want to use controls to avoid waste, fraud, and other issues they may encounter in the course of doing business. The counter to detective controls are corrective controls, which are measures to prevent problems from occurring in the first place.

There are a lot of detective controls can include triggers for certain types of activity, such as warning alerts that will show up when people engage in financial transactions that appear irregular. If a department always issues a check to the same vendor for the same amount, a sudden change might be a cause for concern, and a detective control could be set up to notify the accounting department when variations like this occur so they can find out what happened

- **Preventative controls**

Preventative security controls are put into place to prevent intentional or unintentional disclosure, alteration, or destruction (D.A.D.) of sensitive information. Some example preventative controls follow:

- Policy – It will restrict the unauthorized network connections.

- Firewall – In the firewall, unauthorized

Connections are blocked.

- Locked wiring closet – It is used to prevent unauthorized equipment from being physically plugged into a network switch.[6]

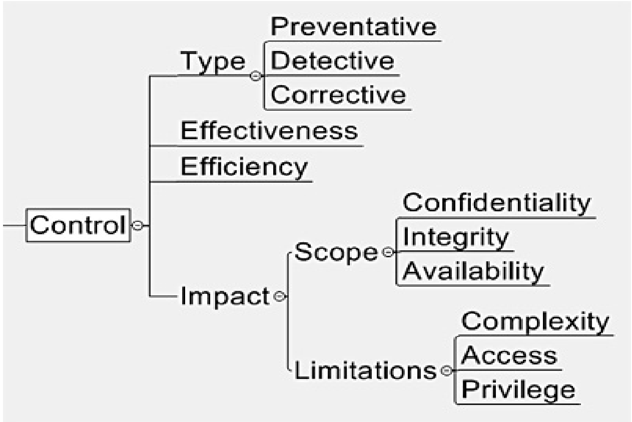


Fig 2.Cloud Security Controls

NEW SECURITY ISSUES

- **Lack of Auditability**

One of the most negative aspects of cloud computing is its ability, or lack thereof, to allow for adequate auditability and to ensure regulatory compliance issues are being addressed. It might surprise some unbelieves that a significant portion of the SaaS community is comfortable with what their service providers offer in that regard.

Audit and compliance issues can vary depending on the type of cloud computing you're considering or implementing. For example, infrastructure-as-a-service generally allows for more control on the part of the customer. On the other hand, software-as-a-service locks down processing on the vendor's site, application features are mostly standard, and customization is generally limited.

- **Regulatory Compliance**

Cloud computing makes it harder for enterprises to be sure they're complying with industry and government regulations. IT and legal experts offer CIOs advice on how to stay in compliance even when their applications reside in the cloud.

Compliance covers a lot of ground, from government regulations such as Sarbanes-Oxley and the European Union Data Protection Act, to industry regulations such as PCI DSS for payment cards and HIPAA for health data. You may have internal controls in place, but moving to a public-cloud infrastructure platform, a cloud-based application suite or something in between will mean giving up some controls to the cloud vendor.[8]

- **No Security Perimeter**

Today's managed security service providers (MSSPs) essentially offer perimeter security management outsourcing. Customers still have to buy and deploy in-premise security equipment such as firewalls, IPD, IDS and the rest. The tedious day to day management and continuous policy process is delegated to the cloud, but the security boxes remain. From that standpoint, today’s managed security services fall short from moving the infrastructure cost and complexity of perimeter security to the cloud.

Another model would be for the PAAS to think as a true platform provider and enable specialized security vendors to start building such services on top of their platform. In that model, MSSPs would start building virtualized, multi-tenant perimeter infrastructure on top of their favorite PAAS, and then, sell perimeter security as a service within these environments to their customer base. Obviously, this would require a different platform than the current MSS infrastructures. Moreover, MSS providers would have to adapt to each specific PAAS, forcing them to make strategic choices and restrict them to a few partners, who may not fit what their customers want in the first place.

- **Larger Attack Surface**

Attack Surface is a measure of how potentially vulnerable a piece of software is. It enumerates the entry points and associated code a malicious user could employ to exploit the software. Examples would be open sockets, RPC entry points, and even the number of web applications hosted inside a web server more programs that are running, the more program code is exposed to malicious users finding vulnerabilities. Also, larger programs will tend to provide more opportunities for exploitation. For example, a web application with 1000 lines of code is generally less likely than a web application with 10000 lines of code to have vulnerability. disabling unneeded features is a good step. In fact, software vendors like Citrix are tending to disable more features by default to improve security. Customers can also disable services and features not used – the smaller the number of features, the less attack surface is effectively available. The principle of least privilege also applies to all deployments.

- **Accountability**

Research has shown that accountability, the ability to reliably monitor the state of a system and faithfully trace its operation, can foster trust in a system by increasing transparency. System transparency enables early detection of faults and malicious behaviors, provides assurances for the compliance to legal and regulatory requirements, and assists in dispute resolution by attributing blame when things go wrong.

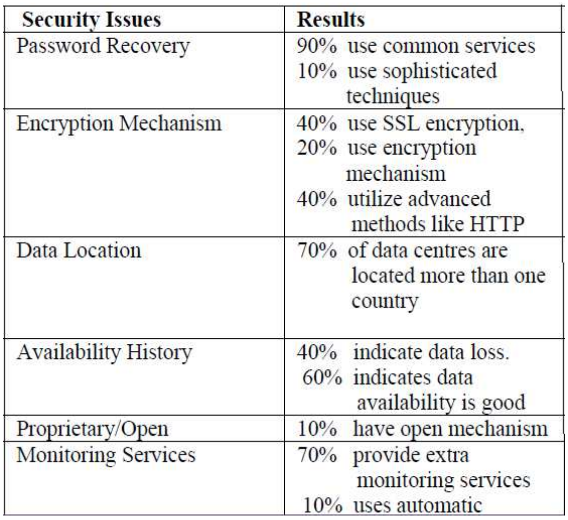
The key challenges lay in the diverse needs of cloud users, the highly dynamic nature of CCS, and the operation over a largely untrusted infrastructure. [9]

Cloud computing introduces a paradigm shift in providing and supporting software services. With this shift come new questions of responsibility and accountability that are highlighted particularly when there is a service outage.

Accountability has clearly undergone some shifts in the cloud, and standards bodies are working to establish outage measurement rules that address the new paradigm. But the rules are not yet in place. For now, some existing distribution of service accountability can be adapted to this new environment.

- **Data Security**

There is also one important security issue "data security" in the data security; we used different techniques to protect data of costumer from the corruption. Following table shows techniques:[9]



Security Issues	Results
Password Recovery	90% use common services 10% use sophisticated techniques
Encryption Mechanism	40% use SSL encryption. 20% use encryption mechanism 40% utilize advanced methods like HTTP
Data Location	70% of data centres are located more than one country
Availability History	40% indicate data loss. 60% indicates data availability is good
Proprietary/Open	10% have open mechanism
Monitoring Services	70% provide extra monitoring services 10% uses automatic

Table 1.Security Techniques for Service Provider

CONCLUSION

This paper has presented the work published by the academic community advancing the technology of cloud computing. Much of the work has focused on different security controls and issues in cloud. This papers firstly working on to prevent customers issues according to security and their control standards..

Various definitions of cloud computing were discussed and the NIST working definition by Mell and Grance [9] was found to be the most useful as it described cloud computing using a number of characteristics, service models and deployment models. The different security technique aspects of cloud computing that were reviewed included the using percentage for privacy to customer. There is a lot of new security issues discussed that are used to focus to protect customers privacy.

You also must be aware of the security risks of having data stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection.

REFERENCES

1. "Swamp computing a.k.a. Cloud Computing". Web Security Journal.2009-12-28. http://security.syscon.com/node/1231725. Retrieved 2010-01-

2. "Thunderclouds: Managing SOA-Cloud Risk". Service Technology Magazine. http://www.servicetechmag.com/I55/1011-1. Retrieved 2011-21-21

3. Gartner (2012) *Cloud Computing*. Retrieved April15,2012from http://www.gartner.com/technology/it-glossary/cloud-computing.jsp

4. Jansen, Wayne & Grance, Timothy. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology, 2011.

5. J Brodkin. (2008). Gartner Seven cloud-computing security risks. http://www.networkworld.com/news/200S!07020Scloud.

6. Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. http://gcn.com/articles/2010/03/18/

dark-cloud-security.aspx. Retrieved 12 February 2012.

7. Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. pp. 59. ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics. http://www.elsevier.com/wps/find/bookdescription.cws_home/723529/description#description

8. YanpeiChen, Vern Paxsonand Randy H. Katz, —What's New about Cloud Computing Security Technical Report No. UCB/EECS-2010-5, http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html, Jan. 20, 2010.

9. NIST, DRAFT Guidelines on Security and Privacy in Public Cloud Computing, http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf , January 28, 2011.